Setting Up Secure Shell

Research Computing Support Group
Division of Information Technology

http://www.rcsg.rice.edu/
<rcsg@rice.edu>
@ricercsg on Twitter

Chandler Wilkerson
chwilk@rice.edu

Joseph Ghobrial
jghobrial@rice.edu
SSH Keys

● `ssh-keygen -t rsa`
  ○ Accept the default `id_rsa` or rename
  ○ Use a password (and `ssh-agent` (Mac, Linux))

● `ssh-copy-id` (Linux only)
  ○ Alternatively, copy `.pub` key to `~/.ssh/authorized_keys` on target account

● Watch the permissions on `~/.ssh` and `$HOME`

● Use an SSH Agent to hold your password protected keys in RAM for your session
SSH Agent Management

$ ssh-add -l

$ eval `ssh-agent`
Agent pid #####

$ ssh-add -l
The agent has no identities.

$ ssh-add
Identity added: /home/netID/.ssh/id_rsa

$ eval `ssh-agent -k`
Agent pid ##### killed;

CSH: eval `ssh-agent -c`
SSH Options

~/.ssh/config

HashKnownHosts yes
Host *.rice.edu
User myNetID
ForwardX11Trusted yes
ForwardAgent yes

Obscure your favorite hosts
Wildcard host stanza
Avoids -l or myNetID@
Automatically include -Y option
Automatically include -A option
See the ssh_config man page for explanations of options
SSH Faster

SSH transfers going slowly? Simplify the encryption overhead by choosing a simpler algo.

$ scp -c arcfour localfile remotefile remote:remotefile

Using rsync?

$ rsync -e "ssh -c arcfour"
SSH Safer

Limit reach of passwordless keys by from="" option in authorized_keys, e.g.

from="192.168.*" ssh-rsa AAAAB3NzaC1yc2E...

Hash known hosts to make it harder to enumerate your favorite hosts

HashKnownHosts yes
Debugging

Sometimes ssh doesn’t work as expected:

```bash
ssh -v   Lots of debug info
ssh -vv  More debug info
ssh -vvv Possibly too much debug info
```